数理解析研究所講究録
第 1806 巻 2012 年 94-98

Some Notes on the Signs of Kloosterman Sums

Wladimir de Azevedo Pribitkin

Let us consider the classical Kloosterman sum

$$A_c(m,n)=\sum_{\substack{a(\bmod c)\\ ad\equiv 1(\bmod c)}} e^{2\pi i\left(\frac{ma+nd}{c}\right)}.$$

Here the numbers m and n are any integers, and the modulus c is a positive integer. $A_c(m,n)$ is a "genuine" Kloosterman sum if $mn\neq 0$, $A_c(m,0)=A_c(0,m)$ is a Ramanujan sum if $m\neq 0$, and $A_c(0,0)$ is simply Euler's totient $\phi(c)$. The significance of Kloosterman sums to the theory of modular forms dates back a century to an astonishingly little-known work of Poincaré [10]. In 1926 Kloosterman [4] published his seminal paper regarding Ramanujan's problem of representing sufficiently large integers by quaternary quadratic forms. Since then these sums have surfaced with an almost unreasonable ubiquity throughout arithmetic.

It is plain that $A_c(m,n)=A_c(-m,-n)$ and hence $A_c(m,n)$ is real. As such, it is natural to ask whether the sequence $\{A_c(m,n)\}_{c=1}^{\infty}$ is oscillatory for fixed integers m and n. That is, are there infinitely many c such that $A_c(m,n)>0$ and infinitely many c such that $A_c(m,n)<0$? Obviously, $\{A_c(0,0)\}_{c=1}^{\infty}$ is positive. And it is clear that $\{A_c(m,0)\}_{c=1}^{\infty}$ is oscillatory for $m\neq 0$ because of the familiar formula (see, for example, [2, p. 238])

$$A_c(m,0)=\mu(\tilde{c})\,\frac{\phi(c)}{\phi(\tilde{c})},$$

where $\tilde{c}=\frac{c}{(c,m)}$ and $\mu(\cdot)$ is the Möbius function. (So as c runs through just the squarefree numbers with at most 2 prime factors, the resulting subsequence is itself oscillatory.) But what if $mn\neq 0$? On the one hand, Kuznetsov's [6] estimate

$$\sum_{1\leq c\leq x}\frac{A_c(m,n)}{c}=O_{m,n}\left(x^{\frac{1}{6}}(\log x)^{\frac{1}{3}}\right) \tag{1}$$

Keywords: Kloosterman sums, oscillatory sequences, Dirichlet series, automorphic forms.

2010 *Mathematics Subject Classification*: Primary 11F30, 11F72, 11L05.

This work was supported (in part) by The City University of New York PSC-CUNY Research Award Program (grant # 64565-00 42).

has often been cited as evidence for the conclusion that cancellation occurs in sums of Kloosterman sums. On the other hand, as apparently pointed out by Serre (see Sarnak's book [14, p. 33] as well as the survey paper by Michel [8, p. 247]), it is plausible that (1) may not be caused by sign changes, but rather be a consequence of all the sums $A_c(m,n)$ being uniformly small for fixed m and n. Nonetheless, Fouvry and Michel [1] (see also [8]) established that $\{A_c(1,1)\}_{c=1}^{\infty}$ is indeed oscillatory. In fact, they proved that as c runs through the squarefree numbers with at most 23 prime factors, the resulting subsequence is oscillatory. They achieved this result by using the theory of automorphic forms coupled with sieve methods and techniques from ℓ-adic cohomology. Subsequently, Sivak-Fischler replaced this number of prime factors by 22 in [16] and then further reduced it to 18 in [17]. And rather recently, Matomäki [7] brought this number down to 15.

Now, is it possible to prove merely that $\{A_c(1,1)\}_{c=1}^{\infty}$ is oscillatory in some simple manner? Yes. By applying the spectral theory of automorphic forms to Selberg's Kloosterman zeta-function

$$Z_{m,n}(s) = \sum_{c=1}^{\infty} \frac{A_c(m,n)}{c^{2s}},$$

it is not difficult to demonstrate the more general result that $\{A_c(m,n)\}_{c=1}^{\infty}$ is oscillatory for any fixed integers m and n such that $mn \neq 0$. We sketch this in a few broad strokes. Evidently, $Z_{m,n}(s)$ is holomorphic for $\sigma = \operatorname{Re} s > 1$. Thanks to the profound work of Selberg [15], it possesses a meromorphic continuation to the whole s-plane. What's more, owing to the fact that the underlying group is $\mathrm{SL}(2,\mathbb{Z})$, $Z_{m,n}(s)$ is holomorphic for $\sigma > 0$ except for the presence of (infinitely many) *nonreal* poles in $0 < \sigma \leq 1/2$. By Landau's Theorem (concerning the abscissa of convergence of Dirichlet series with nonnegative coefficients) this implies immediately that $\{A_c(m,n)\}_{c=1}^{\infty}$ is oscillatory. For further applications of Landau's Theorem to establish the oscillatory behavior of certain sequences arising in number theory, see [5] as well as [11] and [12]. And for more information concerning the analytic behavior of $Z_{m,n}(s)$, please read [6] and [14, pp. 33–41].

But is it possible to prove that $\{A_c(1,1)\}_{c=1}^{\infty}$ is oscillatory in some elementary way? Yes. The main purpose of these notes is to provide an extremely easy proof of the following (more general) result.

Proposition *Let m be any fixed nonzero integer. Then the sequence of Kloosterman sums $\{A_c(m,m)\}_{c=1}^{\infty}$ is oscillatory. Moreover, the following hold:*

(i) For any fixed prime $p \equiv -1 \pmod{4|m|}$, the subsequence $\{A_{p^k}(m,m)\}_{k=2}^{\infty}$ is alternating and $A_{p^2}(m,m) > 0$.
(ii) For any fixed odd integer $k > 1$, the subsequence $\{A_{p^k}(m,m)\}_{p \equiv \pm 1 \pmod{4|m|}}$ is oscillatory. (Here, as usual, p denotes a prime.)

Proof: Since $A_c(m,m) = A_c(|m|,|m|)$, we may suppose that $m > 0$. To begin with, let p be any odd prime such that $(p,m) = 1$ and set $c = p^k$, where $k \geq 2$. By work of Salié [13] from 1931 (for a modern reference, consult [3, p. 60]), we know that

$$A_c(m,m) = 2\left(\frac{m}{c}\right)\sqrt{c}\,\operatorname{Re}\left(\varepsilon_c e^{\frac{4\pi i m}{c}}\right), \tag{2}$$

where $\left(\frac{m}{c}\right)$ is the Jacobi symbol and

$$\varepsilon_c = \begin{cases} 1 & \text{if } c \equiv 1 (\text{mod } 4), \\ i & \text{if } c \equiv -1 (\text{mod } 4). \end{cases}$$

Next, let p be any prime such that $p \equiv \pm 1 (\text{mod } 4m)$. By the Law of Quadratic Reciprocity, it follows easily that $\left(\frac{m}{p}\right) = 1$, and so $\left(\frac{m}{p^k}\right) = 1$.

To prove (i), choose $p \equiv -1 (\text{mod } 4m)$. Since $p^k \equiv (-1)^k (\text{mod } 4)$, we obtain from formula (2) that, for $k \geq 2$,

$$A_{p^k}(m,m) = \begin{cases} 2p^{k/2} \cos\left(\frac{4\pi m}{p^k}\right) & \text{if } k \text{ is even}, \\ -2p^{k/2} \sin\left(\frac{4\pi m}{p^k}\right) & \text{if } k \text{ is odd}. \end{cases}$$

But for some positive integer j, we surely have that $\frac{4\pi m}{p^k} = \frac{\pi(p+1)}{p^k j} \leq \frac{\pi(p+1)}{p^2} \leq \frac{4\pi}{9}$. This implies (i).

To show (ii), take $p \equiv 1 (\text{mod } 4m)$. Because $p^k \equiv 1 (\text{mod } 4)$, we get from (2) that, for any $k \geq 2$,

$$A_{p^k}(m,m) = 2p^{k/2} \cos\left(\frac{4\pi m}{p^k}\right).$$

As before, for some positive integer j, we see that $\frac{4\pi m}{p^k} = \frac{\pi(p-1)}{p^k j} \leq \frac{\pi(p-1)}{p^2} \leq \frac{4\pi}{25}$. Thus, for any fixed integer $k \geq 2$, $\{A_{p^k}(m,m)\}_{p \equiv 1 (\text{mod } 4|m|)}$ is positive. This fact (in conjunction with (i)) establishes (ii). $\square$

Remarks: (i) By Dirichlet's Theorem there exist infinitely many primes p such that $p \equiv 1 (\text{mod } 4|m|)$ and also infinitely many primes p such that $p \equiv -1 (\text{mod } 4|m|)$. (In fact, for such arithmetic progressions "Euclidean proofs" of infinitude are available. For more on such matters, see [9].) (ii) By exploiting Salié's formula (2), we can readily deduce further results. For instance, let m be any fixed nonzero integer and suppose that p is any fixed odd prime such that $(p,m) = 1$. Then it follows that $\{A_{p^k}(m,m)\}_{k=2}^{\infty}$ is oscillatory if and only if $p \equiv -\left(\frac{|m|}{p}\right) (\text{mod } 4)$. What's more, if p satisfies this condition, then $\{A_{p^k}(m,m)\}_{k>k_0}$ is alternating, where k_0 is given by $\max\left\{\frac{\log 8|m|}{\log p}, 1\right\}$. Otherwise, if $p \equiv \left(\frac{|m|}{p}\right) (\text{mod } 4)$, then $\{A_{p^k}(m,m)\}_{k>k_0}$ is positive, with k_0 defined as before. (iii) By core properties of Kloosterman sums, $A_c(m,m) = A_c\left(\frac{m}{\delta}, \delta m\right) = A_c\left(\delta m, \frac{m}{\delta}\right)$, where δ is any divisor of m such that $(\delta, c) = 1$. So the Proposition extends to sums such as $A_c(1, m^2) = A_c(m^2, 1)$.

We conclude by recording a significant special case of the Proposition.

Corollary *The sequence of Kloosterman sums* $\{A_c(1,1)\}_{c=1}^{\infty}$ *is oscillatory. Moreover, the following hold:*

(i) For any fixed prime $p \equiv -1 (\text{mod } 4)$, *the subsequence* $\{A_{p^k}(1,1)\}_{k=2}^{\infty}$ *is alternating and* $A_{p^2}(1,1) > 0$.
(ii) For any fixed odd integer $k > 1$, *the subsequence* $\{A_{p^k}(1,1)\}_{p>2}$ *is oscillatory. (Here, as before,* p *denotes a prime.)*

Remarks: (i) For any fixed integer $k \geq 2$, $\{A_{p^k}(1,1)\}_{p\equiv 1(\mathrm{mod}\ 4)}$ is positive. (ii) A rather challenging (and seemingly intractable) unsolved problem is to establish that $\{A_p(1,1)\}_{p>2}$ is oscillatory.

Acknowledgment: The author thanks Professor Takumi Noda for organizing a rather splendid and highly successful conference at the Research Institute for Mathematical Sciences at Kyoto University in the fall of 2011.

References

[1] É. Fouvry and P. Michel, *Sur le changement de signe des sommes de Kloosterman*, Ann. of Math. (2) 165 (2007), pp. 675–715.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, 5th ed.*, Oxford Univ. Press, Oxford, 1979.

[3] H. Iwaniec, *Topics in Classical Automorphic Forms*, Grad. Stud. Math. 17, Amer. Math. Soc., Providence, RI, 1997.

[4] H. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. 49 (1926), pp. 407–464.

[5] M. Knopp, W. Kohnen, and W. Pribitkin, *On the signs of Fourier coefficients of cusp forms*, Ramanujan J. 7 (2003), pp. 269–277.

[6] N. V. Kuznetsov, *Petersson's conjecture for cusp forms of weight zero and Linnik's conjecture. Sums of Kloosterman sums*, Mat. Sb. (N.S.) 111 (153) (1980), pp. 334–383, Math. USSR Sb. 39 (1981), pp. 299–342.

[7] K. Matomäki, *A note on signs of Kloosterman sums*, Bull. Soc. Math. France 139 (2011), pp. 287–295.

[8] P. Michel, *Some recent applications of Kloostermania*, Physics and Number Theory, ed. L. Nyssen, IRMA Lect. Math. Theor. Phys. 10, Eur. Math. Soc., Zürich, 2006, pp. 225–251.

[9] M. R. Murty and N. Thain, *Primes in certain arithmetic progressions*, Funct. Approx. Comment. Math. 35 (2006), pp. 249–259.

[10] H. Poincaré *Fonctions modulaires et fonctions fuchsiennes*, Ann. Fac. Sci. Toulouse Math. (3) 3 (1912), pp. 125–149.

[11] W. Pribitkin, *On the sign changes of coefficients of general Dirichlet series*, Proc. Amer. Math. Soc. 136 (2008), pp. 3089–3094.

[12] ——, *On the oscillatory behavior of certain arithmetic functions associated with automorphic forms*, J. Number Theory 131 (2011), pp. 2047–2060.

[13] H. Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Z. 34 (1931), pp. 99–109.

[14] P. Sarnak, *Some Applications of Modular Forms*, Cambridge Tracts in Math. 99, Cambridge Univ. Press, Cambridge, 1990.

[15] A. Selberg, *On the estimation of Fourier coefficients of modular forms*, Theory of Numbers (Cal. Tech., Pasadena, CA, 1963), ed. A. L. Whiteman, Proc. Sympos. Pure Math. 8, Amer. Math. Soc., Providence, RI, 1965, pp. 1–15.

[16] J. Sivak-Fischler, *Crible étrange et sommes de Kloosterman*, Acta Arith. 128 (2007), pp. 69–100.

[17] ——, *Crible asymptotique et sommes de Kloosterman*, Bull. Soc. Math. France 137 (2009), pp. 1–62.

DEPARTMENT OF MATHEMATICS
COLLEGE OF STATEN ISLAND, CUNY
2800 VICTORY BOULEVARD
STATEN ISLAND, NEW YORK, 10314 USA
Wladimir.Pribitkin@csi.cuny.edu; w_pribitkin@msn.com